

815 Cryptographic Service Message

Functional Group ID= **CS**

Introduction:

This Draft Standard for Trial Use contains the format and establishes the data contents of the Cryptographic Service Message Transaction Set (815) for use within the context of an Electronic Data Interchange (EDI) environment. The transaction set can be used to provide the data format required for cryptographic key management including the automated distribution and exchange of keys. The mechanism uses X12 structures and data formats and is based on existing standards such as X509 and ANSI X3 and X9 developed by the Accredited Standards Committees (ASCs) X9 and X12. The standard provides an X12 format for key distribution and exchange. The Cryptographic Service Message (CSM) transaction conveys the pertinent keying material for use in the EDI environment. The business requirements addressed in this standard for the key management data encompasses distribution and exchange of keying material in support of authentication, encryption and assurances.

Notes:

This implementation convention supports establishment and conduct of asymmetric security services using public/private keys, where the public portion of the keys is communicated inside an X.509 certificate. When a certification authority (CA) functions within the infrastructure as a peer to the other trading partners, the 815 can be used to request X.509 certificates from the CA. This does not preclude the use of out-of-band exchanges with the CA.

	<u>Pos. No.</u>	<u>Seg. ID</u>	<u>Name</u>	<u>Req. Des.</u>	<u>Max.Use</u>	<u>Loop Repeat</u>	<u>Notes and Comments</u>
Must Use	010	ST	Transaction Set Header	M	1		
Must Use	020	CSM	Cryptographic Service Message Header	M	1		n1
Not Used	030	CSB	Cryptographic Service Message Body	O	>1		
			LOOP ID - CSC			>1	
	033	CSC	Cryptographic Service Message Certificates and Keys	O	1		
	036	DTP	Date or Time or Period	O	9		
Must Use	040	SE	Transaction Set Trailer	M	1		

Transaction Set Notes

1. The CSB segment and the CSC loop are mutually exclusive. If CSM01 = PKS "Public Key Service Message", then the CSC loop shall be used and the CSB segment shall not be used.

Segment: **ST** Transaction Set Header
Position: 010
Loop:
Level:
Usage: Mandatory
Max Use: 1
Purpose: To indicate the start of a transaction set and to assign a control number
Syntax Notes:
Semantic Notes: 1 The transaction set identifier (ST01) used by the translation routines of the interchange partners to select the appropriate transaction set definition (e.g., 810 selects the Invoice Transaction Set).
Comments:

Data Element Summary

	<u>Ref.</u>	<u>Data</u>		<u>Attributes</u>
	<u>Des.</u>	<u>Element</u>	<u>Name</u>	
Must Use	ST01	143	Transaction Set Identifier Code	M ID 3/3
			Code uniquely identifying a Transaction Set	
			815 Cryptographic Service Message	
Must Use	ST02	329	Transaction Set Control Number	M AN 4/9
			Identifying control number that must be unique within the transaction set functional group assigned by the originator for a transaction set	

Segment: **CSM** Cryptographic Service Message Header
Position: 020
Loop:
Level:
Usage: Mandatory
Max Use: 1
Purpose: To indicate the beginning of a Cryptographic Service Message (CSM) Transaction Set and to provide both the class or type of the CSM and the cryptographic end parties to the transaction

Syntax Notes:

Semantic Notes: 1 The three data elements in this segment contain data extracted from the ANSI X9.17 CSM. The correspondence is as follows. CSM01 is the MCL (message class) of the X9.17 CSM. CSM02 is the ORG (originator) of the X9.17 CSM. CSM03 is the RCV (recipient) of the X9.17 CSM.

Comments: 1 These data elements are separated to allow for the recording (logging) of CSMs sent or received and to allow routing to the appropriate security device. The use of these ANSI X9.17 field tags and associated data here is not repeated in the use of the same tags and data in the CSB segments of the detail area of the transaction.
 X12.42 provides strict rules for converting from the ANSI X9.17 CSM to and from the X12.42 CSM and CSB segments. The process is a one-to-one mapping in each direction.

Data Element Summary

Ref.	Data			
<u>Des.</u>	<u>Element</u>	<u>Name</u>		<u>Attributes</u>
Must Use	CSM01	987	Cryptographic Service Message (CSM) Message Class Code Message class (MCL) PKS Public Key Service Message	M ID 3/4
	CSM02	824	Security Originator Name Unique designation (identity) of the cryptographic process that performs authentication or encryption on data to be interchanged, or originates a cryptographic service message Note: X9 has a minimum length of 4 characters for the security originator; no mechanism, or registration method is provided by X9 or X12 to guarantee the uniqueness of the identifier	O AN 1/64
	CSM03	825	Security Recipient Name Unique designation (identity) of the cryptographic process that performs authentication or decryption on received data, or is the destination of a cryptographic service message Note: X9 has a minimum length of 4 characters for the security recipient; no mechanism, or registration method is provided by X9 or X12 to guarantee the uniqueness of the identifier	O AN 1/64

Segment:	CSC Cryptographic Service Message Certificates and Keys
Position:	033
Loop:	CSC Optional
Level:	
Usage:	Optional
Max Use:	1
Purpose:	To provide a mechanism for exchanging certificates of authority, public keys and associated information in an X12 format
Syntax Notes:	<ol style="list-style-type: none"> 1 If any of CSC06 CSC07 CSC08 or CSC09 is present, then all are required. 2 If any of C05005 C05006 C05007 or C05008 is present, then all are required. 3 If any of C05009 C05010 C05011 or C05012 is present, then all are required. 4 If either C04003 or C04004 is present, then the other is required. 5 If either C04005 or C04006 is present, then the other is required.
Semantic Notes:	1 CSC06, CSC07 and CSC08 provide additional information about the encoded security value field in CSC09 (C03302).
Comments:	<ol style="list-style-type: none"> 1 X9 has a required minimum length of 4 characters for CSC02 (security originator). No mechanism, or registration method, is provided by X9 or X12 to guarantee uniqueness of the identifier. 2 X9 has a required minimum length of 4 characters for CSC03 (security recipient). No mechanism, or registration method, is provided by X9 or X12 to guarantee uniqueness of the identifier.

Data Element Summary

Ref.	Data	Attributes
Des.	Element Name	
Must Use	CSC01 1642 Cryptographic Management Purpose	M ID 3/3
	The stated business purpose for exchanging public key on certificate information with a trading partner	
	CCP X509 Certificate Compromised	
	CER X509 Certification Request	
	CEX X509 Certificate Extension	
	CRQ X509 Certificate Request	
	CRT X509 Certificate	
	CRV X509 Certificate Revocation	
	CSR X509 Certificate Status Request	
CSC02	824 Security Originator Name	O AN 1/64
	Unique designation (identity) of the cryptographic process that performs authentication or encryption on data to be interchanged, or originates a cryptographic service message	
	Note: X9 has a minimum length of 4 characters for the security originator; no mechanism, or registration method is provided by X9 or X12 to guarantee the uniqueness of the identifier	
CSC03	825 Security Recipient Name	O AN 1/64

Unique designation (identity) of the cryptographic process that performs authentication or decryption on received data, or is the destination of a cryptographic service message

Note: X9 has a minimum length of 4 characters for the security recipient; no mechanism, or registration method is provided by X9 or X12 to guarantee the uniqueness of the identifier

	CSC04	C050	Certificate Look-up Information	O
			Conveys the information related to or used for certificate identification	
			1. The X.509 Issuer Distinguished Name and Certificate Serial Number will be provided in the CSC04 whenever the CSC01 value is CCP, CER, CEX, or CRV. 2. The X.509 Subject Distinguished Name will be provided whenever the CSC01 value is CRQ or CSR. 3. The X.509 Issuer Distinguished Name and the Subject Distinguished Name will be provided whenever the CSC01 value is CRT.	
Must Use	C05001	1675	Look-up Value Protocol Code	M ID 2/2
			Code specifying the protocol used to identify a certificate	
			AA X509 Issuer Distinguished Name	
			AB X509 Subject Distinguished Name	
			AC X509 Certificate Serial Number	
Must Use	C05002	1570	Filter ID Code	M ID 3/3
			Code specifying the type of filter used to convert data code values	
			HDC Hexadecimal Filter	
			R64 Radix 64	
			UUE UUencoding	
			ZZZ Mutually Defined	
			Use to indicate that NO FILTER is applied to the look-up value	
Must Use	C05003	799	Version Identifier	M AN 1/30
			Revision level of a particular format, program, technique or algorithm	
			If Filter ID Code is ZZZ, then Version Identifier is 'X'.	
Must Use	C05004	1565	Look-up Value	M AN 1/4096
			Value used to identify a certificate containing a public key	
	C05005	1675	Look-up Value Protocol Code	X ID 2/2
			Code specifying the protocol used to identify a certificate	
			AA X509 Issuer Distinguished Name	
			AB X509 Subject Distinguished Name	
			AC X509 Certificate Serial Number	
			ZZ Mutually Defined	
	C05006	1570	Filter ID Code	X ID 3/3
			Code specifying the type of filter used to convert data code values	
			HDC Hexadecimal Filter	

			R64	Radix 64	
			UUE	UUencoding	
			ZZZ	Mutually Defined	
				<i>Use to indicate that NO FILTER is applied to the look-up value</i>	
	C05007	799	Version Identifier	X	AN 1/30
			Revision level of a particular format, program, technique or algorithm		
			<i>If Filter ID Code is ZZZ, then Version Identifier is 'X'.</i>		
	C05008	1565	Look-up Value	X	AN 1/4096
			Value used to identify a certificate containing a public key		
	C05009	1675	Look-up Value Protocol Code	X	ID 2/2
			Code specifying the protocol used to identify a certificate		
			Refer to 004010 Data Element Dictionary for acceptable code values.		
	C05010	1570	Filter ID Code	X	ID 3/3
			Code specifying the type of filter used to convert data code values		
			HDC	Hexadecimal Filter	
			R64	Radix 64	
			UUE	UUencoding	
			ZZZ	Mutually Defined	
				<i>Use to indicate that NO FILTER is applied to the look-up value</i>	
	C05011	799	Version Identifier	X	AN 1/30
			Revision level of a particular format, program, technique or algorithm		
			<i>If Filter ID Code is ZZZ, then Version Identifier is 'X'.</i>		
	C05012	1565	Look-up Value	X	AN 1/4096
			Value used to identify a certificate containing a public key		
Not Used	CSC05	C040	Reference Identifier	O	
			To identify one or more reference numbers or identification numbers as specified by the Reference Qualifier		
Not Used	C04001	128	Reference Identification Qualifier	M	ID 2/3
			Code qualifying the Reference Identification		
			Refer to 004010 Data Element Dictionary for acceptable code values.		
Not Used	C04002	127	Reference Identification	M	AN 1/30
			Reference information as defined for a particular Transaction Set or as specified by the Reference Identification Qualifier		
Not Used	C04003	128	Reference Identification Qualifier	X	ID 2/3
			Code qualifying the Reference Identification		
			Refer to 004010 Data Element Dictionary for acceptable code values.		
Not Used	C04004	127	Reference Identification	X	AN 1/30
			Reference information as defined for a particular Transaction Set or as specified by the Reference Identification Qualifier		

Not Used	C04005	128	Reference Identification Qualifier	X	ID 2/3
			Code qualifying the Reference Identification		
			Refer to 004010 Data Element Dictionary for acceptable code values.		
Not Used	C04006	127	Reference Identification	X	AN 1/30
			Reference information as defined for a particular Transaction Set or as specified by the Reference Identification Qualifier		
	CSC06	1570	Filter ID Code	X	ID 3/3
			Code specifying the type of filter used to convert data code values		
			HDC Hexadecimal Filter		
			R64 Radix 64		
			UUE UUencoding		
			ZZZ Mutually Defined		
	CSC07	799	Version Identifier	X	AN 1/30
			Revision level of a particular format, program, technique or algorithm		
	CSC08	995	Length of Data	X	N 1/18
			Length of data is the number of character positions of the compressed or encrypted/filtered text; when data is plain text, this field shall be absent		
			<i>1. The data in DE1573 is never plaintext; therefore, this value will represent the total number of alphanumeric characters used to represent the filtered X.509 certificate value.</i>		
	CSC09	C033	Security Value	X	
			Value of the Security Token		
Must Use	C03301	1572	Security Value Qualifier	M	ID 3/3
			Type of Security Value		
			CRT Certificate		
Must Use	C03302	1573	Encoded Security Value	M	AN 1/*N/A*
			Encoded representation of the Security Value specified by the Security Value Qualifier		

Segment: **DTP** **Date or Time or Period**
Position: 036
Loop: CSC Optional
Level:
Usage: Optional
Max Use: 9
Purpose: To specify any or all of a date, a time, or a time period
Syntax Notes:
Semantic Notes: 1 DTP02 is the date or time or period format that will appear in DTP03.
Comments:

Data Element Summary				
Ref.	Data			
<u>Des.</u>	<u>Element</u>	<u>Name</u>	<u>Attributes</u>	
Must Use	DTP01	374	Date/Time Qualifier	M ID 3/3
Code specifying type of date or time, or both date and time				
		035	Delivered	
		042	Superseded	
		089	Inquiry	
		102	Issue	
		106	Required By	
		142	Loss	
			When the insured experienced the theft, damage, or casualty to a given property	
		150	Service Period Start	
		151	Service Period End	
		171	Revision	
		177	Cancellation	
			Date on which the coverage or service is no longer in force	
		267	Timenow	
			The current reporting period reference, or current status	
		368	Submittal	
			Date an item was submitted to a customer	
		458	Certification	
			Date of a document attesting to a fact	
		601	First Submission	
		602	Subsequent Submission	
		603	Renewal	
		604	Withdrawn	
		607	Certification Revision	

815A - Cryptographic Service Message (Asymmetric Key)

626	Verified
ABB	Revoked
RRT	Revocation

Must Use	DTP02	1250	Date Time Period Format Qualifier	M ID 2/3
			Code indicating the date format, time format, or date and time format	
			D8	Date Expressed in Format CCYYMMDD
			DTS	Range of Date and Time Expressed in Format CCYYMMDDHHMMSS-CCYYMMDDHHMMSS
Must Use	DTP03	1251	Date Time Period	M AN 1/35
			Expression of a date, a time, or range of dates, times or dates and times	

Segment: **SE** Transaction Set Trailer
Position: 040
Loop:
Level:
Usage: Mandatory
Max Use: 1
Purpose: To indicate the end of the transaction set and provide the count of the transmitted segments (including the beginning (ST) and ending (SE) segments)
Syntax Notes:
Semantic Notes:
Comments: 1 SE is the last segment of each transaction set.

Data Element Summary

	Ref.	Data		
	<u>Des.</u>	<u>Element</u>	<u>Name</u>	<u>Attributes</u>
Must Use	SE01	96	Number of Included Segments	M N0 1/10
			Total number of segments included in a transaction set including ST and SE segments	
Must Use	SE02	329	Transaction Set Control Number	M AN 4/9
			Identifying control number that must be unique within the transaction set functional group assigned by the originator for a transaction set	